EXPLANATORY STATEMENT

Issued by the Authority of the Minister for Finance

Financial Framework (Supplementary Powers) Act 1997

Financial Framework (Supplementary Powers) Amendment (Home Affairs Measures No. 1) Regulations 2024

The *Financial Framework (Supplementary Powers) Act 1997* (the FFSP Act) confers on the Commonwealth, in certain circumstances, powers to make arrangements under which money can be spent; or to make grants of financial assistance; and to form, or otherwise be involved in, companies. The arrangements, grants, programs and companies (or classes of arrangements or grants in relation to which the powers are conferred) are specified in the *Financial Framework (Supplementary Powers) Regulations 1997* (the Principal Regulations). The powers in the FFSP Act to make, vary or administer arrangements or grants may be exercised on behalf of the Commonwealth by Ministers and the accountable authorities of non-corporate Commonwealth entities, as defined under section 12 of the *Public Governance, Performance and Accountability Act 2013*.

The Principal Regulations are exempt from sunsetting under section 12 of the *Legislation (Exemptions and Other Matters) Regulation 2015* (item 28A). If the Principal Regulations were subject to the sunsetting regime under the *Legislation Act 2003*, this would generate uncertainty about the continuing operation of existing contracts and funding agreements between the Commonwealth and third parties (particularly those extending beyond 10 years), as well as the Commonwealth's legislative authority to continue making, varying or administering arrangements, grants and programs.

Additionally, the Principal Regulations authorise a number of activities that form part of intergovernmental schemes. It would not be appropriate for the Commonwealth to unilaterally sunset an instrument that provides authority for Commonwealth funding for activities that are underpinned by an intergovernmental arrangement. To ensure that the Principal Regulations continue to reflect government priorities and remain up to date, the Principal Regulations are subject to periodic review to identify and repeal items that are redundant or no longer required.

Section 32B of the FFSP Act authorises the Commonwealth to make, vary and administer arrangements and grants specified in the Principal Regulations. Section 32B also authorises the Commonwealth to make, vary and administer arrangements for the purposes of programs specified in the Principal Regulations. Section 32D of the FFSP Act confers powers of delegation on Ministers and the accountable authorities of non-corporate Commonwealth entities, including subsection 32B(1) of the FFSP Act. Schedule 1AA and Schedule 1AB to the Principal Regulations specify the arrangements, grants and programs.

Section 65 of the FFSP Act provides that the Governor-General may make regulations prescribing matters required or permitted by the Act to be prescribed, or necessary or convenient to be prescribed for carrying out or giving effect to the Act.

The *Financial Framework (Supplementary Powers) Amendment (Home Affairs Measures No. 1) Regulations 2024* (the Regulations) amend Schedule 1AB to the Principal Regulations to establish legislative authority for government spending on certain activities to be administered by the Department of Home Affairs.

Funding is provided for the following initiatives:

- Supporting an online terrorist crisis response capability to detect and respond 24/7 to online terrorist content and violent terrorist attacks with significant online elements ($2.6 million over four years from 2023-24);
- Enhancing the domestic monitoring and referral capability to identify online terrorist and violent extremist content, and to refer that content to industry ($3.5 million over four years from 2023-24);
- Cyber Awareness—Piloting a Support for Vulnerable Groups Grants Program to uplift the cyber maturity of vulnerable groups through funding grants to community organisations to deliver tailored cyber awareness programs ($9.6 million over three years from 2024-25);
- Information Sharing and Analysis Centre Acceleration Grant Pilot Program to enhance threat sharing capabilities by establishing an Information Sharing and Analysis Centre to enhance cyber security maturity across the health sector ($6.4 million over three years from 2023-24); and
- Professionalisation of the Cyber Workforce Grant Program to develop and test a cyber security professionalisation scheme to enable the recognition of qualifications and experience of professionals in the cyber security industry ($1.9 million over two years from 2023-24).

Details of the Regulations are set out at Attachment A. A Statement of Compatibility with Human Rights is at Attachment B.

The Regulations are a legislative instrument for the purposes of the *Legislation Act 2003*.

The Regulations commence on the day after registration on the Federal Register of Legislation.

Consultation

In accordance with section 17 of the *Legislation Act 2003*, consultation has taken place with the Department of Home Affairs.

A regulatory impact analysis is not required as the Regulations only apply to non-corporate Commonwealth entities and do not adversely affect the private sector.

Attachment A

Details of the *Financial Framework (Supplementary Powers) Amendment (Home Affairs Measures No. 1) Regulations 2024*

Section 1 – Name

This section provides that the title of the Regulations is the *Financial Framework (Supplementary Powers) Amendment (Home Affairs Measures No. 1) Regulations 2024.*

Section 2 – Commencement

This section provides that the Regulations commence on the day after registration on the Federal Register of Legislation.

Section 3 – Authority

This section provides that the Regulations are made under the *Financial Framework (Supplementary Powers) Act 1997*.

Section 4 – Schedules

This section provides that the *Financial Framework (Supplementary Powers) Regulations 1997* are amended as set out in the Schedule to the Regulations.

Schedule 1 – Amendments

Financial Framework (Supplementary Powers) Regulations 1997

Item 1 – In the appropriate position in Part 4 of Schedule 1AB (table)

This item adds five new table items to Part 4 of Schedule 1AB to establish legislative authority for government spending on activities to be administered by the Department of Home Affairs (the department).

New **table item 656** establishes legislative authority for government spending on a program to support an online terrorist crisis response capability to detect and respond 24/7 to online terrorist content and violent terrorist attacks with significant online elements.

On 19 October 2023, the Australian Government announced a series of social cohesion measures to support Australian communities affected by Israel-Hamas conflict (https://minister.homeaffairs.gov.au/ClareONeil/Pages/supporting-australian-communities-affected-hamas-attacks-israel-ongoing-conflict.aspx). This included a $12.8 million package to protect Australians from terrorist and violent extremist online content, comprising:

- supporting a 24/7 online terrorist crisis response capability;
- enhancing the domestic monitoring and referral capability for terrorist and violent extremist content online; and
- providing the eSafety Commissioner additional resources to receive and respond to referrals of abhorrent violent material.

These measures seek to better protect Australians from abhorrent violent material and terrorist and violent extremist content online, particularly in times of heightened global conflict, during terrorist crisis situations, and to minimise harm to Australians and negative impacts on Australia's social cohesion.

Legislative authority through table item 656 is required for funding of $2.6 million over four years from 2023-24 to Tech Against Terrorism to support a 24/7 online terrorist response capability.

The funding intends to address a gap in the global online terrorist crisis response by supporting the expansion of the current crisis response capability of United Kingdom based organisation, Tech Against Terrorism, to operate, both nationally and internationally, continuously covering 24 hours each day. This capability will respond to online terrorist and violent terrorist events that occur both in and outside of Australia.

Tech Against Terrorism is an independent not-for-profit organisation that was launched by the United Nations in 2016, and implemented under their legal entity name the Online Harms Foundation. The organisation consists of an interdisciplinary team of specialists in counter terrorism policy and human rights, open source intelligence analysts, developers and data scientists. The organisation seeks to ensure that tech companies and governments remain vigilant against the online terrorist threat, and aim to empower and educate platforms to improve their existing counter terrorism responses.

Tech Against Terrorism's Terrorist Content Analytics Platform (the Platform) is the largest database of verified digital terrorist content. The Platform is aimed at facilitating tech company moderation of terrorist content and improving quantitative analysis of terrorist use of the internet to aid in preventing and countering this online activity.

The Platform searches for, and alerts digital companies to, terrorist content detected on their platforms. In the case of violent terrorist attacks with significant online elements, such as livestreams, manifestos or other relevant material such as a video or statement produced by the attack perpetrator(s) or their associates, Tech Against Terrorism may activate a crisis response. This includes alerting platforms to online content produced by terrorist attack perpetrator/s, including real time alerting during ongoing crises.

Since the launch of the Platform, Tech Against Terrorism has identified over 43,000 unique URLs, and sent over 24,000 alerts to over 100 tech platforms.

The funding is intended to cover recruitment and employment of Tech Against Terrorism staff in the Australasian region and additional staff in the United Kingdom for a four-year period from 2023-24. These additional staff will provide the capability to respond to online terrorist crisis events in real time, including content alerting and post-incident intelligence briefing. They will also provide briefings outlining trends, developments and key actions taken by Tech Against Terrorism, particularly in Australia, and ongoing engagement with the department.

This will contribute to greater preparedness and ability to respond rapidly to crisis situations as they are unfolding, thereby stemming the onward spread of material after it is uploaded by terrorist attack perpetrators.

The department seeks to undertake a procurement process to support Tech Against Terrorism to undertake activities as outlined above to expand their online terrorist crisis response capabilities to operate on a 24/7 basis.

All procurement related to this activity, including contract amendments, administering the selection process and delegate approvals, will be the responsibility of the department and conducted in accordance with the Commonwealth resource management framework, including the *Public Governance, Performance and Accountability Act 2013* (PGPA Act) and the *Commonwealth Procurement Rules* (CPRs). Final spending decisions will be made by a delegate of the Secretary of the department at the SES level responsible for the management of the activity with the appropriate skills and experience.

Information about the related contracts will be made available on AusTender (www.tenders.gov.au) once these are signed.

Procurement decisions made in connection with supporting a 24/7 online terrorist crisis response capability are not considered suitable for independent merits review, as they are decisions relating to a finite resource, from which all potential claims for a share of the resource cannot be met. Tech Against Terrorism presents a unique capability through their delivery of the Terrorist Content Analytics Platform, which is the largest database of verified online terrorist content. Tech Against Terrorism has been widely recognised by like-minded governments including New Zealand, Canada and the United Kingdom for their expertise in responding to online terrorism, including during crises. The procurement of the services from Tech Against Terrorism will be undertaken in line with the CPRs. Any funding that has already been allocated would be affected if the original decision is overturned.

In addition, independent merits review is not considered suitable for government decisions to allocate funding to programs noting the budgetary decisions for these particular arrangements have been made pursuant to policy interests rather than as a particular decision that affects an individual's interests.

The Administrative Review Council (ARC) has recognised that it is justifiable to exclude merits review in relation to decisions of this nature (see paragraphs 4.11 to 4.19 of the guide, *What decisions should be subject to a merit review?* (ARC guide)).

Consultation with Tech Against Terrorism was undertaken following its proposal for a 24/7 online crisis response capability in the Australasia region. The Christchurch Call has also recommended Tech Against Terrorism to the department as the delivery partner for this capability. The Christchurch Call, jointly run by the governments of France and New Zealand, is a commitment by over 130 governments, online service providers, and civil society organisations to eliminate terrorist and violent extremist content online.

Funding of $2.6 million to support a 24/7 online terrorist crisis response capability was included in the 2023-24 Mid-Year Economic and Fiscal Outlook under the measure 'Supporting Australian Communities Affected by the Hamas-Israel Conflict' for a period of four years commencing in 2023-24. Details are set out in the *Mid-Year Economic and Fiscal Outlook 2023-24, Appendix A: Policy decisions taken since the 2023–24 Budget* at pages 273-274.

Funding for this item will come from Program 1.2: National Security and Criminal Justice and Program 1.4: Counter Terrorism, which are part of Outcome 1. Details are set out in the *Portfolio Additional Estimates Statements 2023-24, Home Affairs Portfolio* at pages 31-32.

Noting that it is not a comprehensive statement of relevant constitutional considerations, the objective of the item references the following powers of the Constitution:

- the communications power (section 51(v)); and
- the external affairs power (section 51(xxix)).

Communications power

Section 51(v) of the Constitution empowers the Parliament to make laws with respect to 'postal, telegraphic, telephonic and other like services'.

Support for an online terrorist crisis response capability will facilitate greater detection and response capabilities for online terrorist content or violent terrorist attacks that have significant online elements or occur on the internet.

External affairs power

Section 51(xxix) of the Constitution empowers the Parliament to make laws with respect to 'external affairs'. The external affairs power supports legislation with respect to matters or things outside the geographical limits of Australia.

The online terrorist crisis response capability will operate nationally and internationally, led by an organisation that operates outside of Australia, with a small physical presence in Australia. This capability will respond to online terrorist events that occur both in and outside of Australia.

New **table item 657** establishes legislative authority for government spending on an expanded domestic monitoring and referral capability for terrorist and violent extremist content online.

On 19 October 2023, the Australian Government announced a series of social cohesion measures to support Australian communities affected by Israel-Hamas conflict (https://minister.homeaffairs.gov.au/ClareONeil/Pages/supporting-australian-communities-affected-hamas-attacks-israel-ongoing-conflict.aspx). This included a $12.8 million package to protect Australians from terrorist and violent extremist online content comprising:

- supporting a 24/7 online terrorist crisis response capability;
- enhancing the domestic monitoring and referral capability for terrorist and violent extremist content online; and
- providing the eSafety Commissioner additional resources to receive and respond to referrals of abhorrent violent material.

These measures seek to better protect Australians from abhorrent violent material and terrorist and violent extremist content online, particularly in times of heightened global conflict, during terrorist crisis situations, and to minimise harm to Australians and negative impacts on Australia's social cohesion.

Legislative authority through table item 657 is required for funding of $1.6 million over four years from 2023-24 to enhance the department's capability to identify and refer terrorist and violent extremist content online by expanding the existing monitoring and referral capability from operating approximately 15 hours per week to approximately 60 hours per week.

Departmental funding of $1.9 million will also be available for the department to implement a data operating model to better record, analyse, report on terrorist and violent extremist data to key stakeholders to inform policy, operational response and engagement with digital industry; and employing additional staff to manage the increase in the referral and reporting of content. Activities delivered under departmental funding are not captured under table item 657.

The department currently maintains a limited domestic capability to monitor and refer terrorist and violent extremist material online. This capability was established under the Combating Terrorist Propaganda measure in 2015-16. The measure was announced in February 2015, with funding of $21.0 million, to limit the impact of extremist narratives on domestic audiences by reducing the support that terrorist groups garner on the internet and social media. This included limiting access to extremist propaganda online through content removal and digital advertising. Between 1 July 2018 and 31 December 2023, 13,859 items of terrorist and violent extremist content were referred by the department to digital industry for consideration for removal against their terms of service. Of these referrals, 9,705 (70 per cent) were removed.

This capability is currently delivered by an external service supplier World Services (Australia) Pty Ltd (trading as M&C Saatchi). The supplier proactively searches for, identifies and refers terrorist and violent extremist content to digital industry for consideration of removal against their terms of service. This includes referring harmful content that is extremely graphic in nature, provides instructions to commit an offence associated with terrorism or expressly promotes or advocates violence against individuals or organisations.

This allows for a set number of hours each week in which the supplier conducts monitoring to identify content and refers content to platforms for consideration under their terms of service for removal. The supplier submits regular reports which are analysed by the department to assess trends on content identification, referral and removal, and ensure referral thresholds are being adhered to.

Currently, this capability operates approximately 15 hours per week. The funding will support an increase in staffing for the supplier to operate for approximately 60 hours a week. A significant increase in these weekly hours is expected to yield a proportionate increase in identification and referral of harmful terrorist and violent extremist content online.

The existing monitoring and referral contract with M&C Saatchi will be varied to allow the delivery of an increased capability in 2023-24. This supplier was selected through a competitive Open Tender using the Digital Transformation Agency's Digital Marketplace Panel (SON3413842) in 2022 to undertake this work for up to a two-year period. The existing contract concludes on 30 June 2024.

From 1 July 2024, expenditure relating to this capability will be undertaken by conducting an Open Tender using the Digital Transformation Agency's Digital Marketplace Panel (SON3413842) to identify and select a supplier to deliver this capability. Procurement decisions will be based on value for money, including capability and capacity to deliver, and price and risk considerations.

All procurement related to this activity, including contract amendments, administering the selection process and delegate approvals, will be the responsibility of the department and conducted in accordance with the PGPA Act and the CPRs. Final spending decisions will be made by a delegate of the Secretary of the department at the SES level responsible for the management of the activity with the appropriate skills and experience.

Information about the related contracts will be made available on AusTender (www.tenders.gov.au) once these are signed.

Procurement decisions made in connection with the domestic monitoring and referral capability are not considered suitable for independent merits review, as they are decisions relating to the allocation of a finite resource, from which all potential claims for a share of the resource cannot be met. Any funding that has already been allocated would be affected if the original decision was overturned.

In addition, independent merits review is not considered suitable for government decisions to allocate funding to programs noting the budgetary decisions for these particular arrangements have been made pursuant to policy interests rather than as a particular decision that affects an individual's interests. The ARC has recognised that it is justifiable to exclude merits review in relation to decisions of this nature (see paragraphs 4.11 to 4.19 of the ARC guide).

The remaking of a procurement decision after entry into a contractual arrangement with a successful supplier is legally complex, impractical, and could result in delays to providing services to platform users. The *Government Procurement (Judicial Review) Act 2018* enables suppliers to challenge some procurement processes for alleged breaches of certain procurement rules. This legislation might provide an additional avenue of redress (compensation or injunction) for dissatisfied suppliers or potential suppliers, depending on the circumstances.

The department engaged with the current supplier M&C Saatchi for this capability to assess their potential capacity expand the existing capability as part of the existing contract due to conclude on 30 June 2024. As the funding objective for the program remains unchanged, the department considers it is not necessary to conduct further consultation.

Funding of $3.5 million for the enhanced domestic monitoring and referral capability for terrorist and violent extremist content online was included in the 2023-24 Mid-Year Economic and Fiscal Outlook under the measure 'Supporting Australian Communities Affected by the Hamas-Israel Conflict' for a period of four years commencing in 2023-24. Details are set out in the *Mid-Year Economic and Fiscal Outlook 2023-24, Appendix A: Policy decisions taken since the 2023–24 Budget* at pages 273-274.

Funding for this item will come from Program 1.2: National Security and Criminal Justice and Program 1.4: Counter Terrorism, which are part of Outcome 1. Details are set out in the *Portfolio Additional Estimates Statements 2023-24, Home Affairs Portfolio* at pages 31-32.

Noting that it is not a comprehensive statement of relevant constitutional considerations, the objective of the item references the communications power (section 51(v)) of the Constitution:

Communications power

Section 51(v) of the Constitution empowers the Parliament to make laws with respect to 'postal, telegraphic, telephonic and other like services'.

The expanded domestic monitoring and referral capability will enable the identification and referral of terrorist and violent extremist content online to digital industry for their consideration for action or removal against their terms of service.

New **table item 658** establishes legislative authority for government spending on the Cyber Awareness—Piloting a Support for Vulnerable Groups Grants Program (the program).

The program will be delivered under the *2023-2030 Australian Cyber Security Strategy* (the Strategy). The Strategy (https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf) supports the department's Program 1.3: Cyber Security within Outcome 1, which is to protect Australia from national security and criminal threats, and support national resilience, through effective national coordination, policy and strategy development and regional cooperation.

The Strategy was announced by the Minister for Home Affairs and Cyber Security on 22 November 2023. Details of the announcement are available at https://minister.homeaffairs.gov.au/ClareONeil/Pages/cyber-strategy-signals-generational-shift-response-growing-threat.aspx.

The Strategy aims to improve Australia cyber security, manage cyber risks and better support individuals and Australian businesses to manage the cyber environment. This is part of the Government's overall objective to ensure that Australia is a world leader in cyber security by 2030.

The Strategy has been developed with Australian citizens and businesses at its core and will take a whole-of-nation approach to building cyber resilience. The Strategy is built around six cyber shields:

1. Strong businesses and citizens;
2. Safe technology;
3. World-class threat sharing and blocking;
4. Protected critical infrastructure;
5. Sovereign capabilities; and
6. Resilient region and global leadership.

The program responds to Shield 1 of the Strategy, which includes action items to ensure Australian citizens and businesses are better protected from cyber threats, and can bounce back quickly following a cyber attack. The program aims to uplift the cyber maturity of vulnerable groups through funding grants to community organisations to develop and deliver tailored cyber awareness programs.

The Government has identified that vulnerable communities are more at risk of being impacted by cybercrime. There is evidence from market research conducted for the *Act Now, Stay Secure* campaign that 55 per cent of the cohort most 'at risk' from cyber threats are female. Research conducted by the Australian Institute of Criminology has suggested that non-binary individuals have been disproportionately impacted by key forms of cybercrime, such as online abuse and harassment; and fraud and scams. The Australian Institute of Criminology has reported that women were less likely to seek help from police or ReportCyber than men. This particular result is supported from demographic data captured in ReportCyber reporting in 2023.

Results from the 2022 Australian Digital Inclusion Index indicates that on a national average basis there is a gap in the digital ability of First Nations people compared with non-Indigenous Australians. This gap is exacerbated for First Nations people in regional and remote Australia. Research conducted by the Australian Institute of Criminology has suggested that First Nations Australians have been disproportionately impacted by all key forms of cybercrime.

The program is intended to be delivered as a pilot. Under the program, the Government has allocated a nominal value for the expected funding per grant. Up to 275 grants will be made available and the value of each eligible funding recipient's allocation has been derived based on estimations of costs to achieve the proposed outcomes, which takes into consideration factors such as population estimates and number of community grants expected across Australia.

Each eligible funding recipient will receive a letter of offer to participate in the program, which will specify their nominal funding allocation. The eligible funding recipient must accept the offer and enter into a grant agreement with the Commonwealth to receive funding up to the nominal funding allocation amount.

Various requirements apply to the funding, including that:

- grant money can only be used on:
    - outreach to vulnerable communities; and
    - eligible expenditure, including developing tailored education materials;
- the projects need to be additional to an eligible funding recipient's existing work plan;
- activity on eligible projects must be undertaken between 1 July 2024 and 30 June 2027; and
- reporting be provided, including on amounts spent, details of progress on projects and jobs supported by the funding, on a quarterly, annual and (where required) ad hoc basis.

To be eligible, applicants must be one of the following entity types:

- Company, incorporated under the *Corporation Act 2001;*
- Cooperative;
- Incorporated Association;
- Indigenous Corporation;
- Local Government Entity, established under state or territory local government legislation, for the purposes of governing local areas within state or territory. In the states, they are generally referred to as local councils;

- Partnership, unincorporated or a non-legal entity and as such, does not have the capacity to enter into a legally binding agreement with the Commonwealth. An individual entity within a partnership must have its own Australian Business Number (ABN) to apply in their own right and be responsible for the terms of the grant agreement, but only if that entity has an eligible entity type as listed above;
- Sole Trader; and
- Statutory Entity, a public enterprise brought into existence by a Special Act of the Parliament. The Act defines its powers and functions, rules and regulations governing its employees and its relationship with government departments. Often these are religious or educational institutions that pre-date the current forms of legal entities.

If an applicant is applying as a Trustee on behalf of a Trust, the Trustee must be one of the eligible entity types as listed above.

Applicants are not eligible to apply if they are a/an:

- Corporate Commonwealth Entity;
- Corporate State or Territory Entity;
- Non-corporate Commonwealth Statutory Authority;
- Non-corporate State/Territory Entity;
- Non-corporate State/Territory Statutory Authority;
- Non-corporate Commonwealth Entity;
- International Entity;
- Person;
- Unincorporated Association;
- Consortium;
- organisation, or the project partner is an organisation, that is included on the National Redress Scheme's website on the list of 'Institutions that have not joined or signified their intent to join the Scheme'; or
- organisation, or the project partner is an organisation, that is included on the Workplace Gender Equality Agency website on the non-compliant list.

Eligible funding recipients will be required to nominate projects they intend to spend grant money on in a work schedule, which will need to be approved before funding is paid. Approval will be based on whether the work schedule complies with the requirements set out in the grant agreement.

The program will be implemented through an open competitive grant process and is expected to commence in August 2024. The program will be delivered over a three-year period with funding to be paid in up to three equal instalments, over the grant period.

The grant will be administered in accordance with the Commonwealth resource management framework, including the PGPA Act and the *Commonwealth Grants Rules and Guidelines 2017* (CGRGs). Grant opportunity guidelines will be developed by the department and together with information about the grant, will be made available on the GrantConnect website (help.grants.gov.au). The grant will be administered by the Community Grants Hub, which is part of the Department of Social Services.

The Community Grants Hub will shortlist applicants and then an assessment panel will provide recommendations to the delegated decision maker in the department.

A delegate of the Secretary of the department under the *Financial Framework (Supplementary Powers) Act 1997* (FFSP Act) will be responsible for final spending decisions on Commonwealth funding provided to grant recipients. Final spending decisions will be made by the Assistant Secretary, Cyber Policy and Programs. In addition, the Assistant Secretary is authorised to approve commitment of relevant money for goods and/or services under the PGPA Act.

Independent merits review is not considered suitable for decisions made in connection with the payments. Funding decisions made at the discretion of the department's delegate can be excluded from independent merits review due to the allocation of finite resource for each financial year from which all potential claims for a share of the resource cannot be met. The ARC has recognised that it is justifiable to exclude merits review in relation to decisions of this nature (see paragraphs 4.11 to 4.19 of the ARC guide).

The Government consulted extensively with stakeholders and industry during the development of the Strategy. A Strategy discussion paper was released on 27 February 2023, with submissions open up to 15 April 2023. The department received over 330 written submissions. Public submissions were published on the department website on 12 September 2023. General feedback supported the need for additional support for Australians in particular at risk vulnerable cohorts.

Funding of $41.9 million over five years from 2023-24 to increase the Australian community's cyber security literacy and awareness through communication and outreach initiatives, including $9.6 million over three years from 2024-25 for the program, was included in the 2023-24 Mid-Year Economic and Fiscal Outlook under the measure '2023-30 Australian Cyber Security Strategy'. Details are set out in the *2023-24 Mid-Year Economic and Fiscal Outlook Appendix A: Policy decisions since the 2023-24 Budget* at page 268.

Funding for the item will come from Program 1.3: Cyber Security, which is part of Outcome 1. Details are set out in the *Portfolio Additional Estimates Statement 2023-24, Home Affairs Portfolio* at page 19.

Noting that it is not a comprehensive statement of relevant constitutional considerations, the objective of the item references the communications power (section 51(v)) of the Constitution.

Communications power

Section 51(v) of the Constitution empowers the Parliament to make laws with respect to 'postal, telegraphic, telephonic and other like services'.

The program will help to expand the national cyber security awareness campaign to uplift cyber security outreach and literacy among the Australian community through developing and delivering tailored cyber security literacy programs.

New **table item 659** establishes legislative authority for government spending on the Information Sharing and Analysis Centre Acceleration Grant Pilot Program (the program).

The program will be delivered under the *2023-2030 Australian Cyber Security Strategy* (the Strategy). The Strategy aims to improve Australia cyber security, manage cyber risks and better support individuals and Australian businesses to manage the cyber environment.

The Strategy has been developed with Australian citizens and businesses at its core and will take a whole-of-nation approach to building cyber resilience. The Strategy is built around six cyber shields:

1. Strong businesses and citizens;
2. Safe technology;
3. World-class threat sharing and blocking;
4. Protected critical infrastructure;
5. Sovereign capabilities; and
6. Resilient region and global leadership.

The program responds to the Strategy under Shield 3: World-class threat sharing and blocking to expand tactical operational threat intelligence sharing. This will ensure that Australia will have access to real-time cyber threat information to block threats at scale.

The program aims to enhance threat sharing capabilities by establishing an Information Sharing and Analysis Centre (ISAC) to enhance cyber security maturity to be piloted in the health sector. ISAC model has been demonstrated to be a scalable and effective model for facilitating industry-to-industry cyber threat intelligence sharing. ISACs provide a structured platform that enables industry participants to collaboratively exchange information. Some industries, such as the Finance and Banking sector have very mature threat sharing capabilities and mature ISACs already operating. Other sectors, such as the health sector, hold large amounts of sensitive data and are less mature in their threat sharing capabilities leaving them more vulnerable. The Government has recognised the need to improve this capability with the health sector ISAC pilot providing an opportunity to enhance and build on existing capabilities with the intention of being able to scale in the future.

Under the program, the Government has allocated a nominal value for the expected funding of the grant. There is one grant available under the program and the value has been determined based on knowledge of the sector and other similar pilot programs. The funding will allow for initial seed funding to build core functions related to intelligence collection and dissemination, member services and governance capabilities.

The eligible funding recipient will receive a letter of offer to participate in program, which will specify their nominal funding allocation. The eligible funding recipient must accept the offer and enter into a grant agreement with the Commonwealth to receive funding up to the nominal funding allocation amount.

Various requirements apply to the funding, including that:

- grant money can only be used to:
    - build core functions related to intelligence collection and dissemination, member services, governance capabilities through establishing a central point

of collection, pooling resources, offering access to threat intelligence feeds and ensuring interoperability and engagement between platforms; and
    - attract membership across industry due to the platform being industry led and enhance the national threat picture as information will be fed into government systems such as the Cyber Threat Intelligence Sharing platform;
- the projects need to be additional to an eligible funding recipient's existing work plan;
- activity on eligible projects must be undertaken between 1 July 2024 and 30 June 2027; and
- reporting be provided, including on amounts spent, details of progress on projects and jobs supported by the funding, on a quarterly, annual and (where required) ad hoc basis.

To be eligible, applicants must:
- have an ABN;
- be registered for the Goods and Services Tax (GST);
- have an account with an Australian financial institution; and
- be an entity, incorporated in Australia.

Joint applications are acceptable, provided the applicants have a lead organisation who is the main driver of the project and is eligible to apply.

Additional eligibility requirements – the applicant's organisation must also be one or more of the following:
- an existing ISAC;
- a health sector group;
- cyber threat specialists; and/or
- a membership organisation for cyber professionals.

Applicants are not eligible to apply if they are:
- an organisation, or their project partner is an organisation, included on the National Redress Scheme's website on the list of 'Institutions that have not joined or signified their intent to join the Scheme';
- an employer of 100 or more employees that has not complied with the *Workplace Gender Equality Act 2012*;
- an individual;
- an unincorporated association;
- a trust (however, an incorporated trustee may apply on behalf of a trust);
- an international entity, unless the submission is a joint application with an Australian entity; or
- any organisation not included in the eligibility criteria.

Eligible funding recipients will be required to outline the key deliverables they intend to spend grant money on in a work schedule, which will need to be approved before funding is paid. Approval will be based on whether the work schedule complies with the requirements set out in the grant agreement.

The program is expected to commence in August 2024. Funding under the program will be paid in up to three instalments, with the first instalment equal to 20 per cent of the recipient's nominal funding allocation in year one to allow for initial establishment of the pilot. The

second and third instalments will be paid over the remaining two years and will each be approximately 40 per cent of the total funding.

The program will be delivered through an open competitive grant process and administered in accordance with the Commonwealth resource management framework, including the PGPA Act and the CGRGs.

Grant opportunity guidelines will be developed by the department and information about the grant will be made available on the GrantConnect website (help.grants.gov.au). The grant will be administered by the Business Grants Hub, which is part of the Department of Industry, Science and Resources.

The Business Grants Hub will shortlist applicants and then an assessment panel will provide recommendations to the delegated decision maker in the department.

A delegate of the Secretary of the department under the FFSP Act will be responsible for final spending decisions on Commonwealth funding provided to grant recipients. Final spending decisions will be made by the Assistant Secretary, Cyber Policy and Programs. In addition, the Assistant Secretary is authorised to approve commitment of relevant money for goods and/or services under the PGPA Act.

Independent merits review is not considered suitable for decisions made in connection with the payments. Funding decisions made at the discretion of the department's delegate can be excluded from independent merits review due to the allocation of finite resource for each financial year from which all potential claims for a share of the resource cannot be met. The ARC has recognised that it is justifiable to exclude merits review in relation to decisions of this nature (see paragraphs 4.11 to 4.19 of ARC guide).

The Government consulted extensively with stakeholders and industry during the development of the Strategy. A Strategy discussion paper was released on 27 February 2023, with submissions open up to 15 April 2023. The department received over 330 written submissions. Public submissions were published on the department website on 12 September 2023. Feedback from consultations indicated that there was general support to increase the threat sharing capabilities across industry through industry-led threat sharing platforms, in particular for low maturity sectors.

Funding of $6.4 million for the program was included in the 2023-24 Mid-Year Economic and Fiscal Outlook under the measure '2023-30 Australian Cyber Security Strategy' over a period of three years commencing in 2023-24. Details are set out in the *2023-24 Mid-Year Economic and Fiscal Outlook Appendix A: Policy decisions since the 2023-24 Budget* at page 268.

Funding for the item will come from Program 1.3: Cyber Security, which is part of Outcome 1. Details are set out in the *Portfolio Additional Estimates Statement 2023-24, Home Affairs Portfolio* at page 19.

Noting that it is not a comprehensive statement of relevant constitutional considerations, the objective of the item references the communications power (section 51(v)) of the Constitution.

Communications power

Section 51(v) of the Constitution empowers the Parliament to make laws with respect to 'postal, telegraphic, telephonic and other like services'.

The program will provide participants with a platform to interact and share information regarding cyber threats on their gateways and networks to reduce cyber security risks.

New **table item 660** establishes legislative authority for government spending on the Professionalisation of the Cyber Workforce Grant Program (the program).

The program will be delivered under the *2023-2030 Australian Cyber Security Strategy* (the Strategy). The Strategy aims to improve Australia cyber security, manage cyber risks and better support individuals and Australian businesses to manage the cyber environment.

The Strategy has been developed with Australian citizens and businesses at its core and will take a whole-of-nation approach to building cyber resilience. The Strategy is built around six cyber shields:

1. Strong businesses and citizens;
2. Safe technology;
3. World-class threat sharing and blocking;
4. Protected critical infrastructure;
5. Sovereign capabilities; and
6. Resilient region and global leadership.

The program responds to the Strategy under Shield 5: Sovereign capabilities, which outlines Australia's vision of a flourishing cyber industry, enabled by a diverse and professional workforce.

The program aims to support the cyber security workforce through building a national professionalisation scheme that will provide employers and businesses with the assurance that the workforce is appropriately skilled, whilst workers know their qualifications and experience are recognised, fit for purpose and support a thriving cyber security ecosystem.

The cyber security industry contributes an estimated $2.4 billion to the economy with significant scope to grow. This industry must be underpinned by a strong cyber workforce to ensure the industry continues to contribute to economic growth and build trust in the digital economy. The industry is lacking clarity in skills qualification and recognition which is a significant barrier for prospective cyber professionals looking to enter the market.

Under the program, the Government has allocated a nominal value for the expected funding of the grant. There is one grant available under the program and the value has been determined based on estimated costs required to engage with the industry and build on existing work undertaken to develop a professionalisation scheme in the industry. Due to lack

of a national framework, a number of jurisdictions and industry leaders have undertaken work in this area, this project would draw on and build on that work.

The funding will be provided over two years to develop and test a cyber security professionalisation scheme in consultation with key stakeholders including cyber security firms, education providers, skills authorities and certifiers. The design of the pilot and scheme would be required to meet core government expectations to examine the ways tertiary qualifications are better aligned with skills needs now and into the future.

Each eligible funding recipient will receive a letter of offer to participate in the program, which will specify their nominal funding allocation. The eligible funding recipient must accept the offer and enter into a grant agreement with the Commonwealth to receive funding up to the nominal funding allocation amount.

Various requirements apply to the funding, including that:

- grant money can only be used to:
    - lead a consortium to develop a professionalisation scheme to ensure clear frameworks for cyber security skills through:
        - a pilot Cyber Security Professionalisation Scheme (the scheme), developed in collaboration with industry, and
        - a plan to scale the scheme after the pilot that provides an increase in industry uptake and participation in the scheme, career pathways for workers in, and seeking to enter, the cyber security workforce, clear guidance for employers and employees regarding skills expectations for accredited professionals, and how the scheme would be self-sustaining and independent from government funding;
    - engage with stakeholders and undertake research to support building the framework, including existing work and skill recognition schemes within the industry. This will include engaging with appropriate industry and accreditation bodies. States and Territories and the Future Skills Organisation;
- the projects need to be additional to an eligible funding recipient's existing work plan;
- activity on eligible projects must be undertaken between 1 July 2024 and 30 June 2026; and
- reporting be provided, including on amounts spent, details of progress on projects and jobs supported by the funding, on a quarterly, annual and (where required) ad hoc basis.

To be eligible, applicants must:

- have an ABN;
- be registered for GST;
- be located in Australia;
- have an account with an Australian financial institution; and
- be an entity, incorporated in Australia.

Joint applications are acceptable, provided the applicants have a lead organisation who is the main driver of the project and is eligible to apply.

Applicants are not eligible to apply if they are:

- an organisation, or their project partner is an organisation, included on the National Redress Scheme's website on the list of 'Institutions that have not joined or signified their intent to join the Scheme';
- an employer of 100 or more employees that has not complied with the *Workplace Gender Equality Act 2012*;
- an individual;
- a Regional Development Australia Committee;
- an unincorporated association;
- a trust (however, an incorporated trustee may apply on behalf of a trust);
- a Commonwealth, state, territory or local government body (including government business enterprises); or
- a non-corporate Commonwealth entity.

Eligibility criteria, including eligible applicants will be set out the program grant opportunity guidelines.

Eligible funding recipients will be required to outline the key deliverables they intend to spend grant money on in a work schedule, which will need to be approved before funding is paid. Approval will be based on whether the work schedule complies with the requirements set out in the grant agreement.

The program is expected to commence in August 2024. Funding under program will be paid in two instalments, with the first instalment equal to 35 per cent of the recipient's nominal funding allocation in year one to allow for initial scoping of the project and establishing scope. The second instalment will be to finalise the development of the framework and undertake a pilot of the scheme.

The program will be delivered through an open competitive grant process and administered in accordance with the Commonwealth resource management framework, including the PGPA Act and the CGRGs.

Grant opportunity guidelines will be developed by the department and information about the grant will be made available on the GrantConnect website (help.grants.gov.au). The grant will be administered by the Business Grants Hub.

A delegate of the Secretary of the department under the FFSP Act will be responsible for final spending decisions on Commonwealth funding provided to grant recipients. Final spending decisions will be made by the Assistant Secretary, Cyber Policy and Programs. In addition, the Assistant Secretary is authorised to approve commitment of relevant money for goods and/or services under the PGPA Act.

Independent merits review is not considered suitable for decisions made in connection with the payments. Funding decisions made at the discretion of the department's delegate can be excluded from independent merits review due to the allocation of a finite resource for each financial year from which all potential claims for a share of the resource cannot be met. The ARC has recognised that it is justifiable to exclude merits review in relation to decisions of this nature (see paragraphs 4.11 to 4.19 of ARC guide).

The Government consulted extensively with stakeholders and industry during the development of the Strategy. A Strategy discussion paper was released on 27 February 2023, with submissions open up to 15 April 2023. The department received over 330 written submissions. Public submissions were published on the department website on 12 September 2023. Stakeholder consultation broadly acknowledged that a prosperous cyber security ecosystem must be built on the foundations provided by a strong domestic cyber security labour market. Feedback supported the idea that the standardisation of cyber professionalisation will create a digitally-skilled workforce that companies are confident in employing.

Funding of $8.5 million over three years from 2023-24 to further grow and professionalise the cyber security industry and support start-ups and small and medium enterprises to innovate and commercialise solutions to cyber security challenges, including $1.9 million over two years from 2023-24 for the program was included in the 2023-24 Mid-Year Economic and Fiscal Outlook under the measure '2023-30 Australian Cyber Security Strategy'. Details are set out in the *2023-24 Mid-Year Economic and Fiscal Outlook Appendix A: Policy decisions since the 2023-24 Budget* at page 268.

Funding for the item will come from Program 1.3: Cyber Security, which is part of Outcome 1. Details are set out in the *Portfolio Additional Estimates Statement 2023-24, Home Affairs Portfolio* at page 19.

Noting that it is not a comprehensive statement of relevant constitutional considerations, the objective of the item references the communications power (section 51(v)) of the Constitution.

Communications power

Section 51(v) of the Constitution empowers the Parliament to make laws with respect to 'postal, telegraphic, telephonic and other like services'.

The program will provide funding to develop and test a cyber security professionalisation scheme. The program will support the development of a workforce with appropriate skills to assist internet users to address cyber security risks by enabling recognition of qualifications and experience of professionals in the industry.

Attachment B

Statement of Compatibility with Human Rights

Prepared in accordance with Part 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011*

Financial Framework (Supplementary Powers) Amendment (Home Affairs Measures No. 1) Regulations 2024

This disallowable legislative instrument is compatible with the human rights and freedoms recognised or declared in the international instruments listed in section 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011.*

Overview of the legislative instrument

Section 32B of the *Financial Framework (Supplementary Powers) Act 1997* (the FFSP Act) authorises the Commonwealth to make, vary and administer arrangements and grants specified in the *Financial Framework (Supplementary Powers) Regulations 1997* (the FFSP Regulations) and to make, vary and administer arrangements and grants for the purposes of programs specified in the Regulations. Schedule 1AA and Schedule 1AB to the FFSP Regulations specify the arrangements, grants and programs. The powers in the FFSP Act to make, vary or administer arrangements or grants may be exercised on behalf of the Commonwealth by Ministers and the accountable authorities of non-corporate Commonwealth entities, as defined under section 12 of the *Public Governance, Performance and Accountability Act 2013*.

The *Financial Framework (Supplementary Powers) Amendment (Home Affairs Measures No. 1) Regulations 2024* amend Schedule 1AB to the FFSP Regulations to establish legislative authority for government spending on certain activities to be administered by the Department of Home Affairs (the department).

This disallowable legislative instrument adds the following table items to Part 4 of Schedule 1AB:

- table item 656 ‘Supporting an online terrorist crisis response capability’;
- table item 657 ‘Expanded domestic monitoring and referral capability for terrorist and violent extremist content online’;
- table item 658 ‘Cyber Awareness—Piloting a Support for Vulnerable Groups Grants Program’;
- table item 659 ‘Information Sharing and Analysis Centre Acceleration Grant Pilot Program’; and
- table item 660 ‘Professionalisation of the Cyber Workforce Grant Program’.

Table item 656 – Supporting an online terrorist crisis response capability

Table item 656 establishes legislative authority for government spending on a program to support an online terrorist crisis response capability (the program).

The program seeks to detect and respond to online terrorist content and violent terrorist attacks with significant online elements that occur both inside and outside Australia. This program will operate nationally and internationally, continuously covering 24 hours each day.

The objective of the program is to better protect Australians from abhorrent violent material and terrorist and violent extremist content online, particularly in times of heightened global conflict and during terrorist crisis situations and minimise harm to Australians and negative impacts on Australia's social cohesion.

Funding of $2.6 million over four years from 2023-24 will be provided to a United Kingdom based independent not-for-profit organisation Tech Against Terrorism (implemented under the legal entity name, the Online Harms Foundation) to deliver the program.

The funding to Tech Against Terrorism will support its expansion of the current crisis response capability to operate, both nationally and internationally, continuously covering 24 hours each day, to detect and respond online to terrorist content and violent terrorist attacks with significant online elements that occur both in and outside of Australia.

Human rights implications

Table item 656 engages the following rights:

- the right to freedom of thought, conscience and religion or belief – Article 18 of the *International Covenant on Civil and Political Rights* (ICCPR), read with Article 2;
- the right to freedom of expression – Article 19 of the ICCPR; and
- the prohibition of propaganda for war and inciting national, racial or religious hatred – Article 20 of the ICCPR.

Right to freedom of thought, conscience and religion or belief

Article 2(1) of the ICCPR requires that each State Party to the Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognised in the Covenant, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.

Article 18 of the ICCPR provides, relevantly:

> 1. Everyone shall have the right to freedom of thought, conscience and religion. This right shall include freedom to have or to adopt a religion or belief of his choice, and freedom, either individually or in community with others and in public or private, to manifest his religion or belief in worship, observance, practice and teaching.
> […]
> 3. Freedom to manifest one's religion or beliefs may be subject only to such limitations as are prescribed by law and are necessary to protect public safety, order, health, or morals or the fundamental rights and freedoms of others.

Table item 656 supports a program to detect and respond to online terrorist content and violent terrorist attacks with significant online elements.

Table item 656 may engage and limit the right to freedom to manifest one's religion or belief if content is religious based terrorist content and, as a result of being detected through this program, is removed from online platforms by the digital content provider. This may affect adherents of particular religions or belief systems at particular times. The aim of this program is to protect the Australian community from abhorrent material and material which may incite violence, and to minimise adverse impacts on social cohesion.

Any limitations on the rights in Article 18(1), including any differential impacts on particular groups, as a result of this program being in place would therefore be reasonable, necessary and proportionate for the purpose of protecting national security, public order, and the fundamental rights and freedoms of others, in accordance with Article 18(3).

Right to freedom of expression

Article 19 of the ICCPR recognises the right to freedom of expression. It provides:

1. Everyone shall have the right to hold opinions without interference.
2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.
3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:
   (a) For respect of the rights or reputations of others;
   (b) For the protection of national security or of public order (*ordre public*), or of public health or morals.

Table item 656 supports a program to detect and respond to online terrorist content and violent terrorist attacks with significant online elements.

Table item 656 may engage and limit the rights to freedom of expression because the program may result in the removal of content posted online by individuals. Further, individuals may choose to not express themselves online as a result of concerns of having their content detected and alerted to digital industry where applicable.

The aim of this program is to protect the Australian community from abhorrent material and material which may incite violence, and to minimise adverse impacts on social cohesion. Any limitations to the rights in Article 19(2) are reasonable, necessary and proportionate for the purpose of protecting national security, public order, and the rights of others, in accordance with Article 19(3).

Prohibition of propaganda for war and inciting national, racial or religious hatred

Article 20 requires States Parties to prohibit, by law, any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence.

Table item 656 supports the objective of Article 20 by enabling programs to detect and respond to terrorist content and violent terrorist attacks with significant online elements that advocates for or incites violence, hostility or discrimination on the basis of nationality, race or religion.

Conclusion

Table item 656 is compatible with human rights because it promotes the protection of human rights.

Table item 657 – Expanded domestic monitoring and referral capability for terrorist and violent extremist content online

New table item 657 establishes legislative authority for government spending to expand the domestic monitoring and referral capability for terrorist and violent extremist content online.

Funding of $1.6 million over four years from 2023-24 is provided to expand the department's capability to identify and refer terrorist and violent extremist content online by increasing the existing monitoring and referral contract from approximately 15 hours per week to approximately 60 hours per week.

The department currently maintains a limited domestic capability to monitor and refer harmful terrorist and violent extremist online. This capability is currently delivered by an external service supplier World Services (Australia) Pty Ltd (trading as M&C Saatchi). The supplier proactively searches for, identifies and refers terrorist and violent extremist content to digital industry for consideration of removal against their terms of service. This includes referring terrorist and violent extremist content that is extremely graphic in nature, provides instructions to commit an offence associated with terrorism or expressly promotes or advocates violence against individuals or organisations.

Currently, this capability operates approximately 15 hours per week. The funding will support an increase in staffing for the supplier to operate for approximately 60 hours a week. A significant increase in these weekly hours is expected to yield a proportionate increase in identification and referral of harmful terrorist and violent extremist content online.

Human Rights Implications

Table item 657 engages the following rights:

- the right to freedom of thought, conscience and religion or belief – Article 18 of the ICCPR, read with Article 2;
- the right to freedom of expression – Article 19 of the ICCPR; and
- the prohibition of propaganda for war and inciting national, racial or religious hatred – Article 20 of the ICCPR.

Right to freedom of thought, conscience and religion or belief

Article 2(1) of the ICCPR requires that each State Party to the Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognised in the Covenant, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.

Article 18 of the ICCPR provides, relevantly:

> 1. Everyone shall have the right to freedom of thought, conscience and religion. This right shall include freedom to have or to adopt a religion or belief of his choice, and freedom, either individually or in community with others and in public or private, to manifest his religion or belief in worship, observance, practice and teaching.
> […]

3. Freedom to manifest one's religion or beliefs may be subject only to such limitations as are prescribed by law and are necessary to protect public safety, order, health, or morals or the fundamental rights and freedoms of others.

Table item 657 supports a program to identify online terrorist and violent extremist content and refer the content to digital industry to consider removal from their platforms.

Table item 657 may engage and limit the right to freedom to manifest one's religion or belief if content is religious based terrorist or violent extremist content and, as a result of being identified through this program, is removed from online platforms by the digital content provider. This may affect adherents of particular religions or belief systems at particular times. The aim of this program is to protect the Australian community from abhorrent material and material which may incite violence, and to minimise adverse impacts on social cohesion.

Any limitations on the rights in Article 18(1), including any differential impacts on particular groups, as a result of this program being in place would therefore be reasonable, necessary and proportionate for the purpose of protecting national security, public order, and the fundamental rights and freedoms of others, in accordance with Article 18(3).

Right to freedom of expression

Article 19 of the ICCPR recognises the right to freedom of expression. It provides:

1. Everyone shall have the right to hold opinions without interference.
2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.
3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:
   (a) For respect of the rights or reputations of others;
   (b) For the protection of national security or of public order (*ordre public*), or of public health or morals.

Table item 657 supports a program to identify online terrorist and violent extremist content and refer the content to digital industry to consider removal from their platforms.

Table item 657 may engage and limit the rights to freedom of expression because the program may result in the removal of content posted online by individuals. Further, individuals may choose to not express themselves online as a result of concerns of having their content monitored and referred to digital industry where applicable.

The aim of this program is to protect the Australian community from abhorrent material and material which may incite violence, and to minimise adverse impacts on social cohesion. Any limitations to the rights in Article 19(2) are reasonable, necessary and proportionate for the purpose of protecting national security, public order, and the rights of others, in accordance with Article 19(3).

Prohibition of propaganda for war and inciting national, racial or religious hatred

Article 20 requires States Parties to prohibit, by law, any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence.

Table item 657 supports the objectives of Article 20 by enabling programs to monitor and refer terrorist or violent extremist content that advocates for or incites violence, hostility or discrimination on the basis of nationality, race or religion.

Conclusion

Table item 657 is compatible with human rights because it promotes the protection of human rights.

Table item 658 – Cyber Awareness—Piloting a Support for Vulnerable Groups Grants Program

Table item 658 establishes legislative authority for government spending on the Cyber Awareness—Piloting a Support for Vulnerable Groups Grants Program (the program).

The program will be delivered under the *2023-2030 Australian Cyber Security Strategy* (the Strategy). The Strategy sets out the Australian Government's vision to be a world leader in cyber security by 2030. The objective of the Strategy is to improve our cyber security, manage cyber risks and better support individuals and Australian businesses to manage the cyber environment.

The Strategy has been developed with Australian citizens and businesses at its core and will take a whole-of-nation approach to building cyber resilience. The Strategy is built around six cyber shields:

1. Strong businesses and citizens;
2. Safe technology;
3. World-class threat sharing and blocking;
4. Protected critical infrastructure;
5. Sovereign capabilities; and
6. Resilient region and global leadership.

The program responds to Shield 1 of the Strategy, which includes action items to ensure Australian citizens and businesses are better protected from cyber threats, and can bounce back quickly following a cyber attack. The program aims to enhance the cyber maturity of vulnerable groups through funding grants to community organisations to develop and deliver tailored cyber awareness programs.

The program is intended to be delivered as a pilot. Grant funding of $9.6 million over three years from 2024-25 is available to support up to 275 grants on:

- outreach to vulnerable communities; and
- developing tailored education materials.

Human Rights Implications

Table item 658 does not engage any of the applicable rights or freedoms.

Conclusion

Table item 658 is compatible with human rights as it does not raise any human rights issues.

Table item 659 – Information Sharing and Analysis Centre Acceleration Grant Pilot Program

Table item 659 establishes legislative authority for government spending on the Information Sharing and Analysis Centre Acceleration Grant Pilot Program (the program).

The program responds to the Strategy under Shield 3: World-class threat sharing and blocking to expand tactical operational threat intelligence sharing. This will ensure that Australia will have access to real-time cyber threat information to block threats at scale.

The program aims to enhance threat sharing capabilities by establishing an Information Sharing and Analysis Centre (ISAC) to enhance cyber security maturity across the health sector. ISACs offer a proven model to support industry-to-industry threat intelligence sharing through its platform where participants interact and share information regarding cyber threats on their gateways and networks.

Grant funding of $6.4 million over three years from 2023-24 will be provided to:

- build core functions related to intelligence collection and dissemination, member services, governance capabilities; and
- attract membership across industry and enhance the national threat picture.

Human Rights Implications

Table item 659 does not engage any of the applicable rights or freedoms.

Conclusion

Table item 659 is compatible with human rights as it does not raise any human rights issues.

Table item 660 – Professionalisation of the Cyber Workforce Grant Program

Table item 660 establishes legislative authority for government spending on the Professionalisation of the Cyber Workforce Grant Program (the program).

The program responds to the Strategy under Shield 5: Sovereign capabilities, which outlines Australia's vision of a flourishing cyber industry, enabled by a diverse and professional workforce.

The program aims to support the cyber security workforce through building a national professionalisation scheme that will provide employers and businesses with the assurance that the workforce is appropriately skilled, whilst workers know their qualifications and experience are recognised, fit for purpose and support a thriving cyber security ecosystem.

The cyber security industry contributes an estimated $2.4 billion to the economy with significant scope to grow. This industry must be underpinned by a strong cyber workforce to ensure the industry continues to contribute to economic growth and build trust in the digital

economy. The industry is lacking clarity in skills qualification and recognition which is a significant barrier for prospective cyber professionals looking to enter the market.

Grant funding of $1.9 million over two years from 2023-24 will be provided to eligible recipient to lead a consortium to develop a professionalisation scheme to ensure clear frameworks for cyber security skills. This also includes engaging with stakeholders and undertake research to support building the framework.

Human Rights Implications

Table item 660 does not engage any of the applicable rights or freedoms.

Conclusion

Table item 660 is compatible with human rights as it does not raise any human rights issues.

Senator the Hon Katy Gallagher
Minister for Finance